Campañas de Phishing se aprovechan del miedo por brote de Coronavirus en el Mundo

El phishing ha sido desde principios de la década de los 2000 el vector de ataque más común empleado por ciber criminales. A medida que las empresas mejoran en la contención y bloqueo de ataques de correo electrónico, los atacantes están cambiando las tácticas, reduciendoel volumen total de ataques y lanzando ataques de phishing más específicos.

Con las recientes noticias sobre la expansión del COVID-19, las diversas organizaciones de delincuentes cibernéticoshan aprovechado el miedo generalizado para realizar campañas de Phishing y Malware dirigidos en nombre de la Organización Mundial de la Salud (OMS) y los Centros para el Control y la Prevención de Enfermedades. Algunos de estos intentos de phishing incluso parecen provenir de correos electrónicos internos de la empresa, con los que pretenden obtener credenciales y detalles de datos bancarios de sus víctimas.

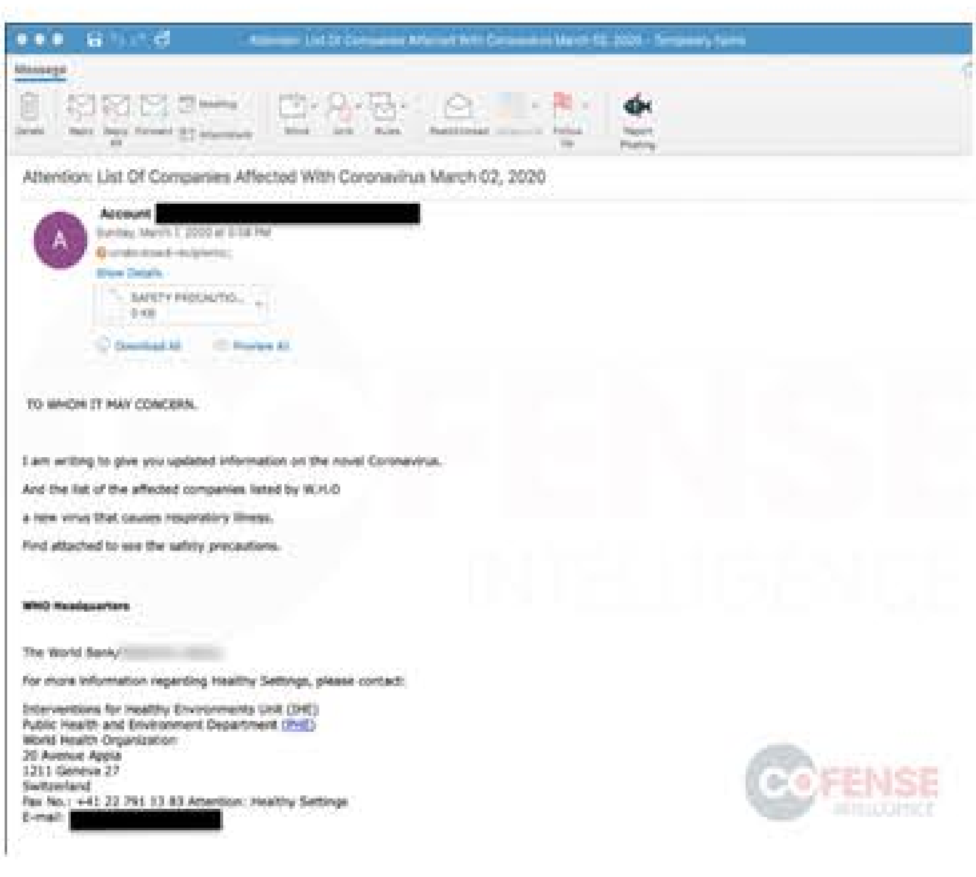
Descripción

Recientemente la compañía Cofense Intelligence™ identificó una campaña de phishing quien suplantando a la Organización Mundial de la Salud (OMS) aprovechó el miedo general para entregar al agente Tesla keylogger quien busca atacar primordialmente la vulnerabilidad CVE-2017-11882.
La campaña de Phishing llevaba como asunto del mensaje “Attention: List Of Companies Affected With Coronavirus March 02, 2020” y tenía como documentos adjuntos los archivos: “Precauciones de Seguridad”, donde el supuesto archivo de Excel (Con el Icono cambiado) correspondía a un ejecutable que desplegaba el agente Tesla Keylogger.

Publicación:
09/03/2020

Importancia:
Alta

Riesgo:
Medio



Attention: List Of Companies Affected With Coronavirus March 02, 2020

Account [redacted]

TO WHOM IT MAY CONCERN,

I am writing to give you updated information on the novel Coronavirus.
And the list of the affected companies listed by W.H.O
a new virus that causes respiratory illness.
Find attached to see the safety precautions.

WHO Headquarters

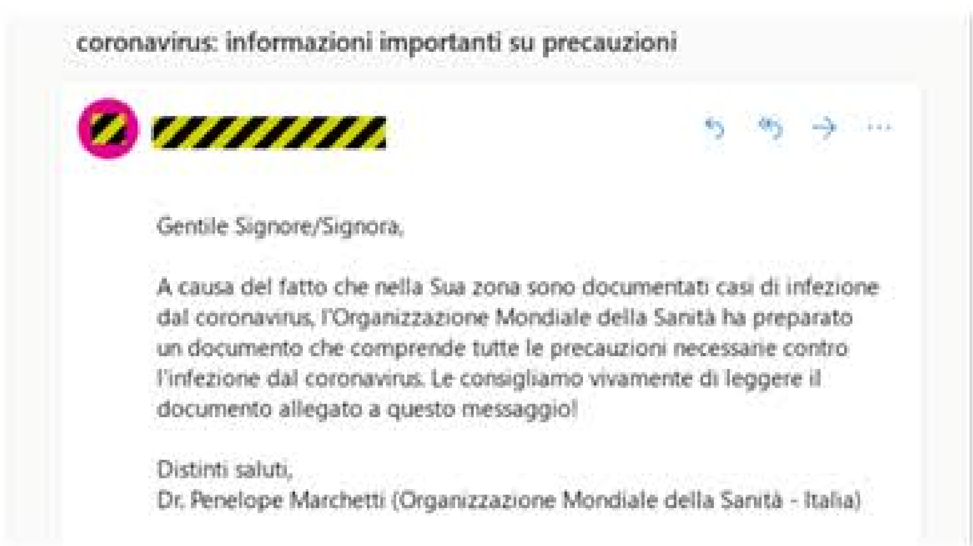
The World Bank/

For more information regarding Healthy Settings, please contact:

Interventions for Healthy Environments Unit (IHE)
Public Health and Environment Department (PHE)
World Health Organization
20 Avenue Appia
1211 Geneva 27
Switzerland
Fax No.: +41 22 791 13 83 Attention: Healthy Settings
E-mail: [redacted]

Recordando que el agente Tesla es un keylogger que data de 2014, tiene funciones de RAT y entre sus funciones se destacan la captura de imágenes desde la cámara web, las técnicas de evasión de antivirus o la posibilidad de descargar nuevos componentes y otras aplicaciones maliciosas, la recopilación de información confidencial, mantener persistencia del ataque, entre otras. La forma más notable en que el Agente Tesla exfiltra los datos robados es a través de correo electrónico; sin embargo, se puede configurar para exfiltrar a través de FTP o un HTTP POST a un punto final .php., este Keylogger está embebido normalmente sobre documentos de la suite MS Office (Word o Excel).

Adicionalmente, los investigadores de Sophos han identificado una campaña de troyanos bancarios Trickbot, dirigida específicamente a direcciones de correo electrónico en Italia, atacando sobre las preocupaciones del virus, este correo electrónico de phishing viene con un documento de Word que pretende dar consejos sobre cómo prevenir la infección, pero este archivo adjunto es de hecho un script de Visual Basic para Aplicaciones (VBA) que deja caer una nueva variante de Trickbot en la máquina de la víctima.



coronavirus: informazioni importanti su precauzioni

[redacted]

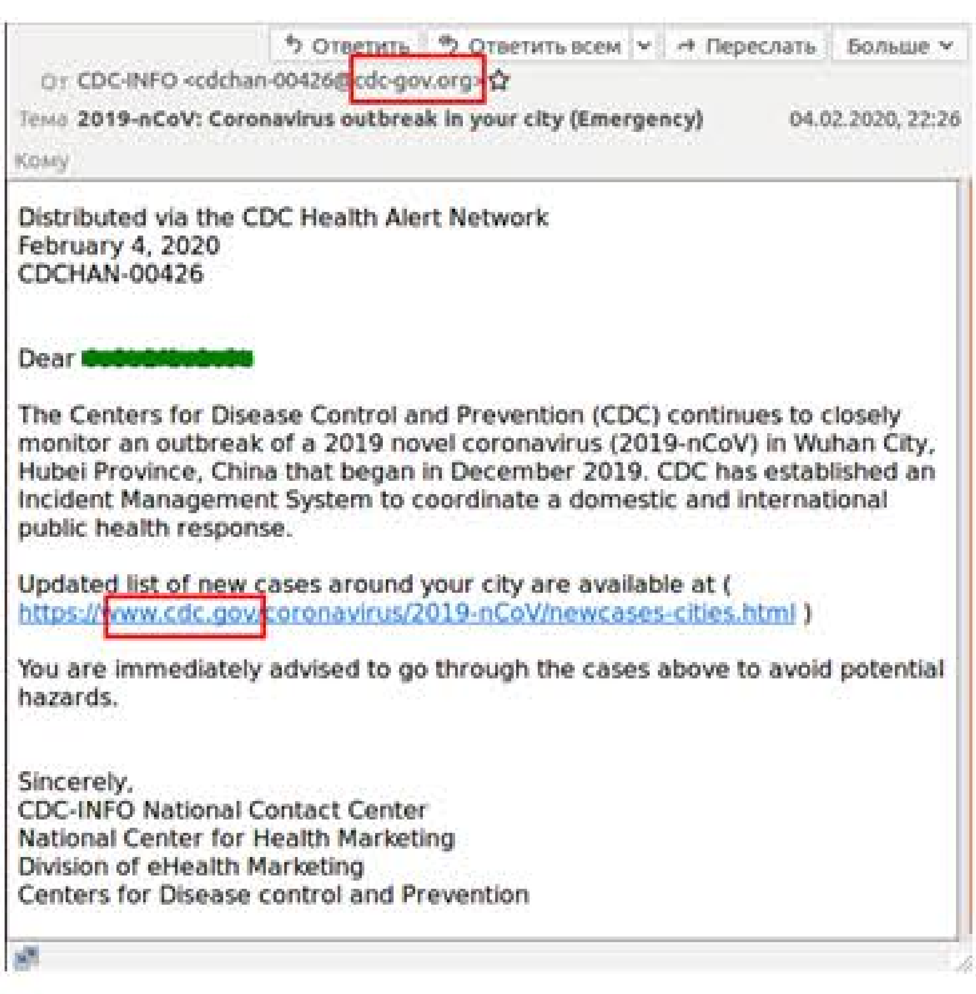
Gentile Signore/Signora,

A causa del fatto che nella Sua zona sono documentati casi di infezione dal coronavirus, l'Organizzazione Mondiale della Sanità ha preparato un documento che comprende tutte le precauzioni necessarie contro l'infezione dal coronavirus. Le consigliamo vivamente di leggere il documento allegato a questo messaggio!

Distinti saluti,
Dr. Penelope Marchetti (Organizzazione Mondiale della Sanità - Italia)

Dentro del correo, un mensaje de alerta falso explica que el archivo fue creado en una versión anterior del software de procesamiento de textos y que es necesario hacer clic en la palabra "activar el contenido" para acceder a todo el documento, acción que luego activa el Malware Trickbot, a continuación, afecta a las redes corporativas interfiriendo en la vulnerabilidad EternalBlue del protocolo SMB (Server Message Block), que permite el uso compartido de recursos en redes locales.

Otros correos con esta misma temática ofrecen un enlace con una supuesta lista de nuevos sospechosos en el área circundante a la que se accedería si se proporcionara una dirección de correo electrónico y una contraseña. Este es un correo electrónico de phishing clásico diseñado para interceptar datos confidenciales.



От CDC-INFO <cdchan-00426@cdc-gov.org>
Тема 2019-nCoV: Coronavirus outbreak in your city (Emergency) 04.02.2020, 22:26
Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

Algo común en todas las compañas de phishing con la temática de coronavirus, es que prometen información sobre las medidas de seguridad para protegerse contra la infección.

PRINCIPAL VECTOR DE ATAQUE: Correo electrónico, enlaces, archivos adjuntos y desbloqueo de Macros para las extensiones de Word- Excel

---

IoC

IP
45[.]128[.]134[.]14

URL

- Insiderppe[.]cloudapp[.]net
- hxxps://45.128.134.14/C821al/vc2Tmy.php?h=m2&j=ffd38fb8&l=NQDPDE@@NQDPDE@@FD1HVy@@*192.168.0.136%3A%3A%5B00000003%5D%20Intel%28R%29%2082574L%20Gigabit%20Network%20Connection&40521390
- kbfvzoboss[.]bid/alien/fre[.]php

HASH MD5
8eb57a3b520881b1f3fd0073491da6c50b7284dd8e66099c172d80ba33a5032f
906EFF4AC2F5244A59CC5E318469F2894F8CED406F1E0E48E964F90D1FF9FD88

HASH SHA-256
ef07feae7c00a550f97ed4824862c459 05adf4a08f16776ee0b1c271713a7880

EMAILS
postmaster@mallinckrodt[.]xyz
brentpaul403@yandex[.]ru

REGLAS YARA
PM_Intel_AgentTesla_36802

Referencias:

https://www.ictjournal.ch/news/2020-03-06/les-campagnes-de-phishing-exploitent-la-peur-du-coronavirus

https://www.fortinet.com/blog/threat-research/attackers-taking-advantage-of-the-coronavirus-covid-19-media-frenzy.html

https://en.mogaznews.com/Technology/1456870/Hackers-are-disguising-phishing-attacks-as-official-emails-from-public-health-.html

https://www.zdnet.com/article/nasty-phishing-scams-aim-to-exploit-coronovirus-fears/

https://www.vox.com/recode/2020/3/5/21164745/coronavirus-phishing-email-scams

https://www.kaspersky.es/blog/coronavirus-phishing/21059/

Recomendaciones

- Ejecutar programas de concientización al personal sobre los últimos ataquesde phishing / spearphishing .
- No hacer click a links ni abrir archivos adjuntos en correos sospechosos y no confiar en correos de remitentes desconocidos.
- Actualización continua del antivirus e IPS. Si se considera que la aplicación de parches no es factible, se recomienda realizar una evaluación de riesgos para determinar salvaguardas de mitigación adicionales dentro de un entorno.
